REMARKS

Original claims 1-21 have been examined. No claims have been allowed. The specification has been amended, independent claims 4, 6, 10, 15, and 18 have been amended, and new claims 22, 23, and 24 have been added in this amendment. Applicants appreciate the examiner's time and the courtesy extended during the March 4, 2003 telephonic interview with applicants' representative, Grace Law. The substance of the interview is set forth in the Examiner's Interview Summary Record, which is of record as Paper No. 6. Favorable reconsideration of claims 1-24 is requested in view of the following remarks.

In the Office action mailed January 10, 2003, claims 4-6, 10, 15, 17, and 18 are rejected for allegedly being anticipated by U.S. Patent No. 6,269,410 B1 to Spasojevic (hereinafter "Spasojevic"). The remaining claims 1-3, 7-9, 11-14, 16, and 19-21 are rejected for allegedly being obvious over Spasojevic.

The Office action states that one of ordinary skill in the art at the time the invention was made would have known that the transport layer interfaces for communicating between processes and other devices, making it obvious that the detecting step occurs at the transport layer of the protocol stack (Office action, page 5). For the following reasons, applicants assert that Spasojevic neither describes nor suggests the detecting of a transmission or reception of data in the transport-layer as recited in the claims, and as will be described in greater detail below.

One skilled in the relevant art will appreciate that there are at least seven layers in an open network system: (1) a physical layer, (2) a data link layer, (3) a network layer, (4) a transport layer, (5) a session layer, (6) a presentation layer, and (7) an application layer (Attachment C).

The present invention provides traces of data traffic on a network at the transport layer of the TCP/IP stack, which allows for discrimination among various types of transmission (Applicants' specification, page 2, lines 7-10). Specifically, the transport layer establishes and dissolves connections between hosts (see Attachment A). A host is a computer connected to a network (Attachment B). Devices such as routers and printers are not normally referred to as hosts (Attachment B). In particular, since only the Input/Output Request packets (IRP) representing sends and receives are detected as the IRP pass through the stack, there is no need to continuously track the network activity by protocol type and the service port number (Applicants' specification, page 2, lines 10-13). For example, a TCP Send is traced at the end of the send (Applicants' specification, page 6, line 17), since only the completion of a TCP Send is noteworthy and the use of the NIC to send out the number of bytes is guaranteed (Applicants' specification, page 6, lines 27-31). For a TCP Receive, a trace is recorded when a first chunk of data is received and when the Receive operation is complete (Applicants' specification, page 7, lines 11-17). Thus, unlike the network sniffer used in the prior method, the present invention does not require continuous tracking of the data flow. Rather, only the completion of the TCP

Send and the first chunk of data along with the completion of the TCP Receive are tracked. As a result, the trace method of the present invention is able to discriminate among and record only desired events.

To the contrary, Spasojevic is limited to teaching tracing data flow between a server 14a and one or more hard drives 24 in a data storage system connected over a network (FIG. 1; Col. 1, line 66 to Col. 2, line 2; Col. 3, lines 49-53). In this regard, Spasojevic simply describes conventional tracing of data flow on a network, which is similar to a network sniffer. Because Spasojevic is limited to teaching connections between a computer and a peripheral device, such as a hard drive, a printer, or a router, it fails to teach or suggest connections on the transport layer relating to connections between hosts (e.g., two computers). Thus, Spasojevic fails to teach or suggest tracing data flow in the transport layer of a host in an open network system. Further, Spasojevic fails to teach or suggest tracing data flow in the host-to-host transport layer of the TCP/IP stack for detecting a transmission or reception of data to and from other hosts.

The following remarks are grouped to reflect the organization of the Office action.

Section 102 rejection – Claims 4-6, 10, 15, 17, and 18

Claims 4-6, 10, 15, 17, and 18 are rejected under 35 U.S.C. §102(e) as being anticipated by Spasojevic. Claims 4-6, 10, 15, 17, and 18 include independent claims 4, 6, 10, 15, and 18. In response, applicants amended claims 4, 6, 10, 15, and 18 to include

the feature of "a transport-layer request" to overcome the rejection. Nothing in Spasojevic discloses or suggests such a feature. This rejection should be withdrawn.

Section 103 rejection – Claims 1-3, 7-9, 11-14, 16, and 19-21

Claims 1-3, 7-9, 11-14, 16, and 19-21 are rejected under 35 U.S.C. §103(a) as being unpatentable over Spasojevic. Claims 1-3, 7-9, 11-14, 16, and 19-21 include independent claims 1 and 12. Each of those claims recites the feature of "at the transport layer of a protocol stack residing on a first device in the network, detecting a transmission or receipt of data to or from a second device on the network." Nothing in Spasojevic discloses or suggests such a feature. In particular, Spasojevic's tracing of data between a host (e.g., a computer) and a peripheral device (e.g., a hard drive, a printer, or a router) at the physical layer is substantially different from tracing data traffic between hosts on the transport layer. By tracing data at the transport layer, the traces allow discrimination among types of data. By tracing at the physical layer, Spasojevic only suggests indiscriminating recording of the data traces. Thus, nothing from the cited reference suggests the detecting step at the transport layer as recited in independent claims 1 and 12. Dependent claims 2-3, 7-9, 11, 13-14, 16, and 19-21 include the same detecting step of the independent claims and, therefore, are patentable for at least the same reasons as independent claims 1, 6, 10, 12, 15, and 18, from which they respectively depend. For all these reasons, the Section 103 rejection of claims 1-3, 7-9, 11-14, 16, and 19-21 should

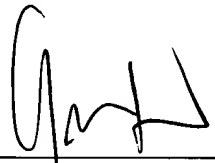
be withdrawn.

CONCLUSION

In view of the above amendments and remarks, the application is considered in good and proper form for allowance, and the examiner is respectfully requested to pass this application to issue.

If, in the opinion of the examiner, a telephone conference would expedite the prosecution of the subject application, the examiner is invited to call the undersigned attorney.

Respectfully submitted,



Grace Law, Reg. No. 48,872
One of the Attorneys for Applicant(s)
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
180 North Stetson
Chicago, Illinois 60601-6780
(312) 616-5600 (telephone)
(312) 616-5700 (facsimile)

Date: April 10, 2003

transport layer

<*networking*> (Or "host-host layer") The middle layer in the OSI seven layer model. The transport layer determines how to use the network layer to provide a virtual error-free, point to point connection so that host A can send messages to host B and they will arrive un-corrupted and in the correct order. It establishes and dissolves connections between hosts. It is used by the session layer.

An example transport layer protocol is Transmission Control Protocol (TCP).

OSI documents: ITU Rec. X.214 (ISO 8072), ITU Rec. X.224 (ISO 8073).

(1997-12-07)

Try this search on OneLook / Google

Nearby terms: transparent « transparent audio coding « Transport Driver Interface « **transport layer** » Transport Layer Interface » Transport Level Interface » Transport Service Access Point

---

" ATTACHMENT A "

host

1. <*networking*> A computer connected to a network.

The term node includes devices such as routers and printers which would not normally be called "hosts".

2. <*communications*> A computer to which one connects using a terminal emulator.

(1995-02-16)

Try this search on OneLook / Google

Nearby terms: hose « hosed « HOS-STPL « **host** » host adaptor » Host Command Facility » Host Control Interface

---

"ATTACHMENT B"

means of FTP from nis.nsf.net, nisc.jvnc.net, venera.isi.edu, wuarchive.wustl.edu, src.doc.ic.ac.uk, ftp.concert.net, internic.net, or nic.ddn.mil.

TCP/IP Protocol Architecture

TCP/IP protocols map to a four-layer conceptual model known as the DARPA model, named after the U.S. government agency that initially developed TCP/IP. The four layers of the DARPA model are: Application, Transport, Internet, and Network Interface. Each layer in the DARPA model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) model.

Figure 1 shows the TCP/IP protocol architecture.

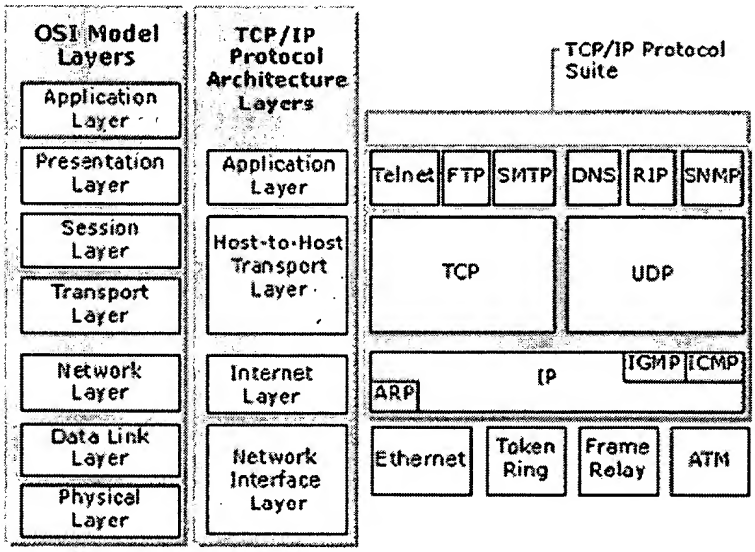


Figure 1. TCP/IP protocol architecture

Network Interface Layer

The Network Interface Layer (also called the Network Access Layer) is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets from the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. In this way, TCP/IP can be used to connect differing network types. This includes LAN technologies such as Ethernet or Token Ring and WAN technologies such as X.25 or Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).

The Network Interface Layer encompasses the Data Link and Physical layers of the OSI Model. Note that the Internet Layer does not take advantage of sequencing and acknowledgment services that may be present in the Data Link Layer. An unreliable Network Interface Layer is assumed, and reliable communications through session establishment and the sequencing and acknowledgment of packets is the responsibility of the Transport Layer.

Internet Layer

The Internet Layer is responsible for addressing, packaging, and routing functions. The core protocols of the Internet Layer are IP, ARP, ICMP, and IGMP.

- The Internet Protocol (IP) is a routable protocol responsible for IP addressing and the fragmentation and reassembly of packets.
- The Address Resolution Protocol (ARP) is responsible for the resolution of the Internet Layer address to the Network Interface Layer address, such as a hardware address.
- The Internet Control Message Protocol (ICMP) is responsible for providing diagnostic functions and reporting errors or conditions regarding the delivery of IP packets.

"ATTACHMENT C"